



SAVONIA

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
TEKNIIKAN JA LIIKENTEEN ALA

ACTIVE DIRECTORY MIGRAATIOPROJEKTI JA OFFICE 365 KÄYTTÖÖNOTTO

TEKIJÄ/T: Niko Hotari

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Niko Hotari	
Työn nimi Active Directoryjen yhdistäminen sekä Office 365 käyttöönotto	
Päiväys 29.05.2020	Sivumäärä/Liitteet 33/0
Ohjaaja(t) Pasi Liimatainen	
Toimeksiantaja/Yhteistyökumppani(t) Best Friend Group Oy / Janne Iivanainen	
<p>Tiivistelmä</p> <p>Työn aiheena oli dokumentoida tilaajan IT-ympäristön päivitys, sisältäen kahden Active Directoryn yhdistämisen ja migroinnin, sekä Office 365 käyttöönoton syksyn 2019 sekä talven 2020 aikana. Työssä kuvataan projektin lähtökohta, projektin aikana suoritettavat menetelmät ja tärkeimmät tapahtumat sekä lopputulos. Työn valmistuttua tilaaja voi tarkistaa dokumentista projektissa toteutetut muutokset, sekä konsultoida ongelmanratkaisutilanteissa.</p> <p>Tilaajan IT-ympäristön todettiin olevan päivityksen tarpeessa ja päivitys päätettiin toteuttaa yhtenä isona projektina, sisältäen kuitenkin kaksi selkeästi erottuvaa osiota. Tilaajan Active Directory migroitiin uuteen ympäristöön yritysmuutoksista johtuen. Käytiin läpi yrityksen käyttäjälistaa siivoten samalla käyttämättömiä tilejä sekä pohtien mahdollisia Active Directoryn rakennemuutoksia.</p> <p>Tilaajalla oli käytössä Exchange 2007-sähköpostipalvelin, joka toi migraatioon lisähaasteita. Sähköpostilaatikoiden migraatio 2007-versiosta 2016-versioon ei ole tuettu suoraan, joten tilaajan ympäristöön luotiin lisäksi myös Exchange 2013-serveri. Exchange 2013 toimi tässä vaiheessa vain migraation välikappaleena sillä migroitavat kohteet jäivät serverille enimmillään muutamiksi tunneiksi. Testaus suoritettiin testikäyttäjien ja laitteiston avulla, pyrkien huomioimaan kaikkien työntekijöiden mahdolliset eri tilanteet. Näin saatiin näkemys sekä toimistolla, että VPN-yhteydellä toimivien käyttäjien migraatiotuloksista.</p> <p>Office 365:n toiminnan perusvaatimus on Azure Active Directoryn käyttöönotto, sillä kyseessä on hybridimalli jossa palveluita on sekä pilvessä, että paikallisessa ympäristössä. Serverille asennettiin työkalu, jolla paikallisia objekteja synkronoitiin pilvessä sijaitsevaan Azure Active Directoryyn. Tämän jälkeen voitiin siirtyä lisenssien hallintaan, jonka jälkeen Office 365 voitiin asentaa ja ottaa käyttöön.</p> <p>Lopputilanteessa ympäristön tärkeimmät vaiheet saatiin suoritettua, mutta koronan vuoksi projekti keskeytyi ja osa vaiheista jäi odottamaan myöhempää ajankohtaa. Active Directory ja sähköpostilaatikot saatiin migroitua sekä Office 365 otettua käyttöön, mutta laitteisto ja serverit sijaitsevat edelleen vanhassa ympäristössä. Lisäksi Active Directory-rakenteen suunnittelu muutoksineen jäi toteuttamatta.</p>	
<p>Avainsanat</p> <p>Office 365, Active Directory, Exchange, migraatio, käyttöönotto</p>	

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Niko Hotari			
Title of Thesis Active Directory Migration and Establishing Office 365			
Date	29 May, 2020	Pages/Appendices	33/0
Supervisor(s) Mr. Pasi Liimatainen, Senior Lecturer			
Client Organisation /Partners Best Friend Group Oy / Janne Iivanainen			
<p>Abstract</p> <p>The purpose of this thesis was to document the client's migration project. The project consisted of three phases. The first was the migration of Active Directory objects. The second was the migration of mailboxes. The last phase was to introduce Office 365 across company. The client can consult this document in problem solving instances.</p> <p>Active Directory and mailbox migrations began with testing. The migration tasks themselves were done, which were performed with the necessary tools. Active Directory migration was performed from a server built for it from the old environment. The mailbox migration was performed from an Exchange server in the new environment. The mailbox migration had some challenges which the team overcame. The final phase consisted of implementing Office 365. The first step was to build a server to sync on-premise Active Directory objects to the cloud. After this licenses were assigned, and the software was installed for the users.</p> <p>As a result of this thesis, most of the environment was successfully migrated. The coronavirus ended the project pre-maturely, leaving hardware and server migration to be done at a later date. However, the main goal was to migrate users and mailboxes, in which the project was successful.</p>			
Keywords Office 365, Active Directory, Exchange, migration, establishment			

ESIPUHE

Tahdon kiittää Best Friend Groupin IT-päällikköä Janne Iivanaista mahdollisuudesta osallistua projektiin, jonka tuloksena tämä opinnäytetyö tuotettiin. Lisäksi tahdon kiittää Best Friend Groupin Antti Hyväristä työn aikana tarjotusta palautteesta ja näkökulmista. Viimeisenä tahdon kiittää Savonia-ammattikorkeakoulun Pasi Liimataista ohjauksesta työn aikana.

Kuopiossa 29.5.2020

SISÄLTÖ

1	JOHDANTO	7
2	TYÖN TOTEUTUS JA KUVAUS	7
3	BEST FRIEND GROUP OY	8
3.1	Yritys	8
3.2	Historia	8
3.3	Liiketoiminta	8
3.4	Motivaatio ympäristöpäivitykselle	8
4	TEORIA	9
4.1	Active Directory	11
4.2	Exchange	12
4.3	Sähköpostipalvelut hybridi-mallissa.....	13
4.4	IaaS – Infrastructure as a service.....	13
4.5	PaaS – Platform as a Service	14
4.6	Microsoft Azure	14
4.7	Microsoft 365.....	15
4.8	Azure Active Directory.....	15
4.9	Autodiscovery	16
5	YMPÄRISTÖN LÄHTÖTILANNE	17
6	PROJEKTIN KÄYTÄNNÖN TOTEUTUS	18
6.1	Suunnittelu.....	18
6.2	Uudet serverit.....	18
6.3	Trustien rakentaminen	19
6.4	Active Directory-migraatio	20
6.5	Exchange-migraatio.....	20
6.5.1	Testaus	22
6.5.2	Mobiililaitteiden migrointi	22

6.5.3	Kannettavien migrointi.....	23
6.5.4	Migraation jälkeiset ongelmat.....	23
6.6	Sähköpostin uudelleenreititys	24
6.7	Office 365 migrointi.....	24
6.8	Office 365 käyttöönotto	25
6.8.1	Office 365-lisenssit.....	25
6.8.2	Asennus.....	26
6.8.3	Käyttäjien opastus	26
6.8.4	Käyttöönoton jälkeiset ongelmat.....	26
6.9	Group Policy Object-päivitykset.....	27
7	KORONAN VAIKUTUKSET	27
7.1	Laitteistomigraatio.....	27
7.2	Exchange Online-migratio	28
7.3	Serverimigraatio.....	29
8	POHDINTA.....	30
9	LÄHTEET JA TUOTETUT AINEISTOT	32

1 JOHDANTO

Opinnäytetyön aiheena on kuvata projektia, jonka tavoitteena on kahden Active Directoryn migraatio uuteen ympäristöön sekä Office 365 käyttöönotto tilaajalle, Best Friend Groupille. Opinnäytetyössä kuvataan tilaajan ympäristön lähtötilanne, haluttu lopputulos, sekä menetelmät joilla haluttu lopputulos saavutettiin. Mahdollisesta opinnäytetyöstä keskusteltiin kesällä 2018 työharjoittelun ohessa, ja oli selvää että tämä projekti oli nousemassa ajankohtaiseksi.

Tilaajan ympäristö on ajautumassa tilanteeseen, jossa tuki on loppumassa, joten oli selvää että tämä projekti olisi erittäin ajankohtainen. Lisäksi yrityksellä on edessä laajoja organisaatiomuutoksia yhdistymisestä johtuen, joten palveluiden on mukauduttava tilanteeseen sopivaksi. Yrityksillä on päällekkäisyyksiä toimintatavoissa ja työkaluissa, mutta myös eriävyyksiä, joita pyritään purkamaan projektiin liittyvillä ratkaisuilla.

Työ suoritettiin lokakuu 2019 – maaliskuu 2020 välillä, ja projektiryhmään sisältyi lisäksi BFG:n kaksihenkinen IT-tiimi Kuopiossa, yksi VPG:n työntekijä Tanskassa, sekä ulkopuolinen palvelinasiantuntija joka palkattiin projektiluontoisesti avuksi. Käytännön perspektiivistä katsoen BFG:n ja VPG:n tietohallinto oli yksi työryhmä, sillä heillä oli jo valmiiksi yhteisiä sähköposteja mm. IT-tukea varten, jaettu Teams-työtila yhteydenpitoon sekä tiedostojen ja informaation jakamiseen.

2 TYÖN TOTEUTUS JA KUVAUS

Työhön sisältyi käytännön osuus tilaajan toimistolla Kuopiossa, sekä opinnäytetyön kirjallinen osuus joka ei ole sijaintiin sidonnainen. Opinnäytetyössä kuvataan tilaajan ympäristön tämän hetkinen tilanne, lopputulos, sekä menetelmät joilla lopputulokseen päästiin.

Järjestyksessä ensimmäisenä oli serverien rakentaminen uuteen ympäristöön, josta siirryttiin ensimmäisenä migroimaan kummankin yrityksen käyttäjät. Oli selvää että Active Directoryn käyttäjämigraatio, sekä Exchange-serverin sähköpostilaatikot on järkevää hoitaa ensin, jonka jälkeen Office 365 otettaisiin yhteisesti käyttöön molempien sijaitessa yhteisillä servereillä. Ennen Office 365 käyttöönottoa määriteltiin Azure Active Directory-synkronointi paikallisen Active Directoryn kanssa, sillä tämä on pakollinen Office 365:n toiminnalle hybridiympäristössä. Office 365 käyttöönotto toteutettiin osastoittain IT:stä alkaen, jotta mahdollisiin ongelmakohtiin on helpompi tarttua, sekä niiden vaikutukset rajattua. Lisäksi Office 365-asennus vaati manuaalisen asennuksen, tarkoittaen että jonkun paikallisesta projektiryhmästä oli oltava läsnä asennuksen yhteydessä.

Työn tukemiseen käytettiin materiaalia verkosta sekä tilaajalta luvan nojalla. Viisihenkinen projektiryhmä piti säännöllisesti palvereita, joissa kirjattiin projektin tavoitteita ja toimia. Kokonaisuus toteutettiin pienempiä valmisteluita lukuunottamatta edellisessä kappaleessa kuvatussa järjestyksessä.

3 BEST FRIEND GROUP OY

3.1 Yritys

Best Friend Group Oy syntyi, kun tanskalaisomistuksessa oleva VPG jakautui kahtia keväällä 2008. Best Friend Groupiin siirtyi yhtiön omilla tuotemerkeillä harjoitettava liiketoiminta, kun taas kaupan omilla merkeillä tapahtuva valmistus jäi tanskalaisyhtiöön.

Best Friend Groupin pääkonttori sijaitsee Kuopiossa, ja yhtiöllä on tytäryhtiöt Tanskassa, Ruotsissa ja Norjassa. Yhtiön logistiset toiminnot on keskitetty Kuopioon ja Århusiin (Tanska). Konsernin palveluksessa on noin 120 työntekijää.

3.2 Historia

Best Friend Groupin historia juontaa juurensa vuoteen 1973, jolloin Taisto ja Tapio Kuusela perustivat yhtiön nimeltään Puijon Nahkatuote Ay. 1980-luvulla yhtiön nimi muuttui Kerox Oy:ksi. Kerox Oy vaihtoi omistajaa vuonna 1997, jolloin yhtiön omistajaksi tuli CapMan Oy rahastoineen, Erkki ja Marjaana Moisander sekä Mika Sutinen. Tanskalainen Vital Petfood Group osti Kerox Oy:n vuonna 2000, jolloin yhtiön nimi muuttui VPG Finland Oy:ksi. Keväällä 2008 yhtiön nimi muutettiin Best Friend Group Oy:ksi mukaellen yhtiön päätuotemerkkiä "Best Friend."

3.3 Liiketoiminta

Best Friend Group Oy:n liiketoiminta keskittyy lemmikkieläintarvikkeiden kehittämiseen, markkinointiin ja jakeluun. Kaksi keskeisintä jakelukanava ovat suuret päivittäistavaraketjut sekä erikoistuneet lemmikkieläinkaupat ja -ketjut, joita palvelee molemmille erikseen räätälöidyillä tuotevalikoimilla.

Päivittäistavarakaupalle yhtiö toimittaa laajan valikoiman Best Friend -tuotteita koirille, kissoille sekä muille lemmikkieläimille. Tuotevalikoima kattaa lemmikkien ja lemmikkien omistajien tarvitsemat perustarvikkeet koko lemmikin elinkaarelle. Päätuotteet ovat koirien makupalat, puruluut, kissanruoka sekä kissanhiekka.

Erikoistavarakauppaa harjoittava Hurtt & Co keskittyy palvelemaan asiakkaitaan muun muassa Hurtt ja Racinel -tuotteilla.

Best Friend Group Oy on lemmikkitarvikkeiden selkeä markkinajohtaja Pohjoismaissa. Tavoitteena on kasvaa johtavaksi toimijaksi eurooppalaisessa mittakaavassa seuraavan viiden vuoden aikana.

3.4 Motivaatio ympäristöpäivitykselle

Yrityksellä on pitkään ollut sisaryhtiön asema tanskalaisen Vital Petfood Groupin (VPG) kanssa, ja yhdistyminen nousi ajan myötä tarpeelliseksi ratkaisuksi. Kahden yrityksen yhdistyessä yhteiseksi

nimeksi vaihtuu Nordic Petcare Group. Opinnäytetyössä keskitytään BFG:n puoleen, mutta ajoittaista kuvausta VPG:n puolelta ei voida välttää, sillä sama viiden hengen projektiryhmä hoiti molempien yritysten migraatiota identtisin ratkaisuin.

4 TEORIA

Osiossa esitellään tärkeimmät lyhenteet, sekä teoreettinen lähestymistapa ja tehtäväjärjestys projektin toteuttamiselle.

Active Directory migraation tärkeimmät työvälineet ovat seuraavat:

AD = Active Directory, käsitellään tarkemmin teoriaosiossa.

NPC = Nordic Petcare, viittaa työssä uuteen ympäristöön ja siellä sijaitseviin palveluihin ja servereihin.

ADMT = Active Directory Migration Tool. Microsoftin tarjoama serverille asennettava työkalu, joka on suunniteltu migraatiota varten.[2]

PES = Password Export Server. Microsoftin tarjoama serverille asennettava työkalu, joka on suunniteltu tuomaan käyttäjien salasanat vanhasta ympäristöstä uuteen.[3]

Domain = Verkkotunnus. Esim www.google.fi tai www.savonia.fi

Domain/Forest trust = Valmistelutoimenpide, joka sujuvoittaa migraation toteutumista kahden eri domainin välillä. [2]

FQDN = Fully Qualified Domain Name. Käytetään verkkosivustoilla ja servereillä kun halutaan määritellä kohde tarkemmin. Vaaditaan usein migraatitöissä. Usein muodossa www.google.fi tai serveri1.bestfriend.com

PowerShell = käyttökehote tyylinen työkalu, jolla voidaan suorittaa erinäisiä käskyjä. Voidaan käyttää migraatiovaiheissa graafisen käyttöliittymän sijaisena jos halutaan lisää hallintaa.

OU = Organizational Unit, käyttäjäryhmä jota voidaan hyödyntää hallinnallisessa ja tietoturva mielessä.

GPO = Group Policy Object, tarjoaa lisäkontrollia AD-käyttäjille ja laitteistoille.

Yksi tapa toteuttaa kahden Active Directoryn migraatio on seuraava:

1. Luodaan luottamus (Domain/Forest trust) kahden eri domainin välillä
2. Valmistellaan salasanojen tuontityökalu (PES)
3. Luodaan migraatioserveri
4. Valmistellaan käyttäjäkoneet sekä uusi domain migraation aloittamista varten
5. Migroidaan käyttäjät uuteen ympäristöön (ADMT)
6. Migroidaan koneet uuteen ympäristöön (ADMT) / päivitetään käyttäjäluvat uuteen ympäristöön sopivaksi
7. Kopioidaan sähköpostilaatikat uuteen ympäristöön
8. Korjataan Outlook osoittamaan uuden ympäristön sähköpostiserverille [2]

Office 365 käyttöönoton tärkeimpiä termejä:

Cutover migration = Migrintitapa, jossa kaikki sähköpostilaatikat siirretään kerralla. Sopii pienille yrityksille. [1]

Staged migration = Migrintitapa, jossa kaikki sähköpostilaatikat siirretään vaiheittain. Ei sisällä suoraa tukea Exchange 2007:lle, joka tilaajalla on käytössä.[4]

DNS = Domain Name System. Kääntää verkkotunnuksia IP-osoitteiksi.

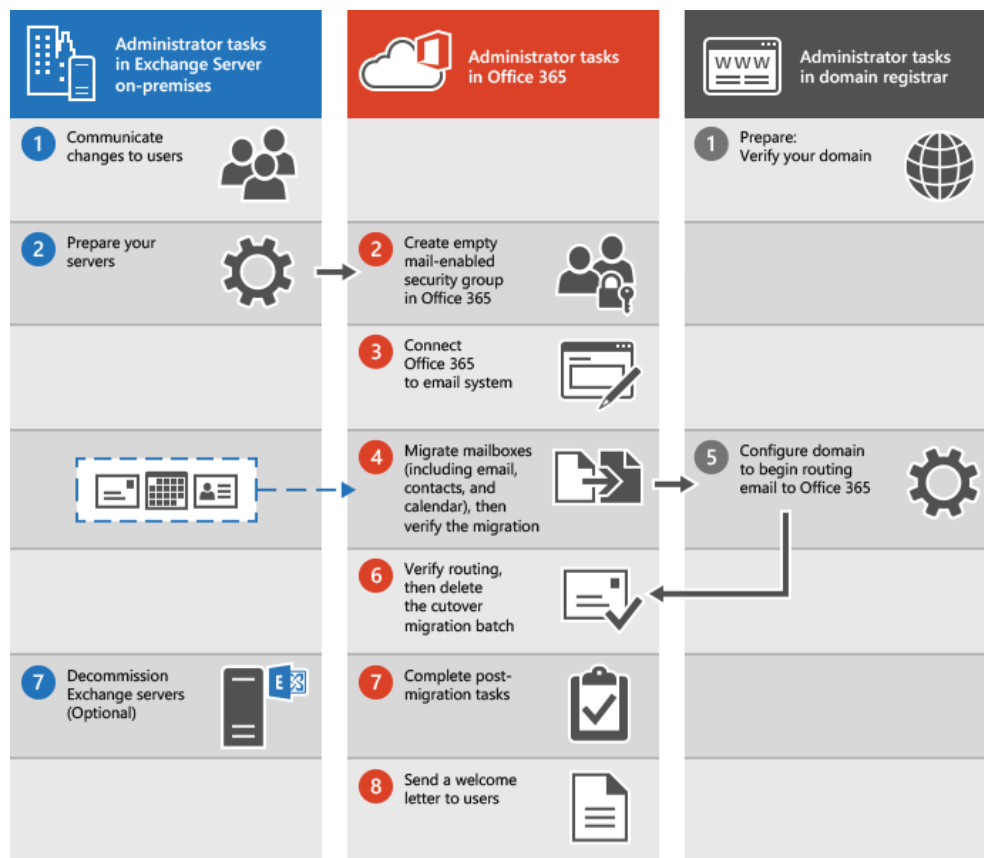
TXT record = Tiedosto, jolla vahvistetaan domainin omistajuus. Hankitaan DNS-palveluntarjoajalta.[1]

Migration batch = Työ, joka käynnistetään migraation suorittamiseksi.[1]

EAC = Exchange Admin Console, paikallisen on-premise serverin hallintaan käytettävä web-pohjainen hallintapaneeli.

ECP = Exchange Control Panel, pilvessä sijaitsevan Exchange Online serverin hallintaan käytettävä web-pohjainen hallintapaneeli.

Oheisessa kuvassa kuvataan askeleiden avulla tiivistetysti Office 365:n käyttöönotto Cutover migraatiota hyödyntämällä.



Kuva 1. Office 365:n pääaskeleet [1]

Pääaskeleet ovat siis seuraavat:

1. Kommunikoidaan muutokset käyttäjille / Vahvistetaan domainin omistajuus
2. Valmistellaan serverit migraatiota varten / Luodaan tyhjä turvallisuusryhmä Office 365:n hallintapaneelista
3. Yhdistetään Office 365 sähköpostijärjestelmään
4. Suoritetaan migraatio, ja vahvistetaan toimivuus
5. Määritetään domain reitittämään sähköposti Office 365
6. Vahvistetaan sähköpostireitityksen toimivuus sekä poistetaan migraatiotyö
7. Suoritetaan migraation jälkeiset tehtävät / poistetaan paikallinen Exchange serveri käytöstä.
8. Toivotetaan käyttäjät tervetulleeksi uuden palvelun pariin

Työn voi jakaa kolmeen vaiheeseen. Alkutilanteessa kuvataan yrityksen nykyinen ympäristörakenne, sekä motivaatio päivitykselle. Menetelmissä kuvataan projektin edetessä kuvatut toimintatavat, joilla halutut päivitykset saatiin suoritettua. Lopputilanteessa pohditaan menetelmien onnistumista.

4.1 Active Directory

Aktiivihakemisto (Active Directory). Looginen rakennelma, joka säilyttää verkossa olevaa informaatiota. Näihin lukeutuvat mm. verkossa sijaitsevat käyttäjät, laitteistot sekä serverit. Hakemiston työkaluilla voidaan säilyttämisen lisäksi hallita pääsyä verkossa olevaan dataan ja resursseihin. Hakemistossa säilytetään informaatiota käyttäjätileistä, kuten nimet, salasanat ja

puhelinnumerot, ja samalla voidaan hallinnoida kansiopääsyjä esim. osastoittain organisaation sisällä. Hakemiston on suotavaa noudattaa loogista rakennetta työkalujen ja toiminnan takaamiseksi, sillä näin taataan sujuva yhteistyö muiden palveluiden kanssa. Näihin sisältyvät mm. ryhmäkäytännöt, työpöydän mahdollinen sulkeminen, ohjelmiston jako, sekä käyttäjien, ryhmien, päätteiden sekä servereiden hallinnointi. [6]

Hakemistoon kuuluu neljä tärkeintä elementtiä, jotka toimivat kaiken toiminnan perustana. Schema sisältää määrittelyt jokaiselle hakemistossa sijaitsevalle objektille rajoituksineen. Näihin sisältyvät sekä adminien itse luomat kohteet, että scheman vaatimat toiminnalle pakolliset objektit. Scheeman sisältö eritellään luokkiin ja ominaisuuksiin, joilla hakemiston tietoa jaotellaan. Globaali katalogi sisältää tietoa hakemiston jokaisesta objektista. Tämän avulla admin pystyy hakemaan kohteita hakemiston sisällä niiden loogisesta sijainnista huolimatta, olivat ne missä tahansa. [6]

Kysely- ja indeksimekanismien avulla objektit pystyvät löytämään toisensa hakemistosta. Näitä hyödyntävät sekä käyttäjät, että sovellukset. Palvelu eritellään haku- ja julkistuskomponentteihin. Hakukomponentti käsittelee hakupyyntöjä, ja julkistuskomponentti mahdollistaa objektien tietojen jakamisen itsestään.

Replikaatiopalvelu ylläpitää hakemistossa sijaitsevaa tietoa koko verkon tasolla. Kaikki toimialueen hallitsijaserverit osallistuvat tähän prosessiin, ja niistä jokaisessa on kopio koko hakemistosta tietoineen. Samalla hakemistoon tehdyt muutokset replikoituvat muihin hallitsijaservereihin. [6]

Hakemistoa hallitaan sille tarkoitetuilla työkaluilla (Active Directory Domain Services). Tämän avulla admin pystyy järjestelemään hakemistossa sijaitsevaa informaatiota loogisiin hierarkisiin kokonaisuuksiin. Hakemiston hierarkinen rakenne on aina seuraava: Metsä (forest). Metsä yhdistää useita toimialueita, ja toimii näin hakemiston korkeimmalla tasolla. Saman metsän alla olevia toimialueita yhdistävät looginen rakenne, luokka ja ominaisuusrajoitukset, replikaatioinformaatio sekä globaali katalogi. Metsään sisältyvät toimialueet linkitetään aina molempiin suuntiin toimivalla luottamus-suhteella.

Toimialue (domain). Toimialueen avulla osioidaan metsään sisältyvät kokonaisuudet loogisesti esim. organisaation toimipisteiden mukaan. Tämä auttaa hakemiston hallinnoinnissa, ja replikoinnissa datan toimiessa siinä loogisessa kokonaisuudessa johon se kohdistuu estäen datavuodon muille alueille. Lisäksi toimialue-tasolla hallitaan hakemiston tärkeitä ominaisuuksia, kuten käyttäjien identiteettihallintaa, autentikointia sekä toimialueiden luottamussuhteita. [7]

Organisaatioyksikkö (Organisational unit/OU). Organisaatioyksiköillä jaotellaan toimialueen sisäisiä objekteja kokonaisuuksiin, esim. organisaation sisäisiin osastoihin. Näiden avulla pystytään hallitsemaan käyttäjien pääsyä resursseihin kuten verkkohakemistoihin. [7]

Exchange-serveri on vastuussa sähköpostiin liittyvistä tehtävistä, sekä organisaation sisällä kuin ulkopuolella. Exchange-kokonaisuus koostuu kahdesta eri roolista, joihin kuuluvat Mailbox ja Edge Transport-roolit. [8]

Mailbox-osioon kuuluu tietokanta, joka prosessoi ja säilyttää sähköpostidataa. Lisäksi välissä on front-end palvelu, joka käsittelee ja reitittää palvelimelle tulevia käyttäjäyhteyksiä ja protokollia. Servereitä hallinnoidaan Exchange Admin Center (EAC), sekä Exchange Management Shell työkaluilla. [8]

Edge transport-serveri on vastuussa postin kuljettamisesta organisaation verkon ulkopuolelle. Serveri saa aktiivihakemistosta EdgeSync-synkronointiprosessin avulla tiedon määrittämisestä, sekä vastaanottajatiedoista yksisuuntaista replikaatiota hyödyntäen. Lisäksi serverin tehtäviin kuuluu roskapostilta suojaaminen, sekä postin reitittämiseen liittyvät säännöt. Serveri sijoitetaan yleensä verkon ”ulkoreunalle” toimien näin erillään, sekä suojaten samalla sisäverkkoa. Kyseinen serveri ei yleensä kuulu organisaation Active Directoryyn loogisen sijoittelunsa vuoksi. Serveri päästää läpi sisäverkkoon ainoastaan viestejä jotka läpäisevät niille asetetut ehdot, ja se etsii vastaavuuksia datan, sanallisten kaavojen, otsikon, liitettyypin tai lähettäjäsähköpostin perusteella. [8]

Exchange-palveluun kuuluu database availability group (DAG)-elementti, jonka tehtävä on kasvattaa serverin sietokykyä erinäisiä virhetilanteita vastaan. Käytännössä tähän kuuluu tietokannan palautus tietokanta-, verkko-, tai serveriongelmien sattuessa. DAG koostuu useasta Mailbox-serveristä, mahdollistaen näin palautuksen. [8]

4.3 Sähköpostipalvelut hybridi-mallissa

Hybridimallissa palvelut on hajautettu paikallisille Exchange-servereille, sekä Azuren pilvipalveluun. Käyttäjien postilaatikot sijaitsevat edelleen paikallisessa Exchange-serverillä, josta ne synkronoidaan Azuren pilvipalveluun. Käyttäjille ulospäin näkyy käytännössä vain yksi palvelu, sillä komponentit toimivat käytännössä yhtenä ja käyttäjät kirjautuvat molempiin yhtenäisillä tunnuksilla. Postilaatikon ja Office 365:n tunnuksat ovat tässä tapauksessa samat. [11]

4.4 IaaS – Infrastructure as a service

IaaS-palvelussa palveluntuottaja tarjoaa infrastruktuuria palveluna asiakkaalle tyypillisesti niin, että asiakkaan käyttöön tarjotaan web-pohjainen hallintaliittymä, jonka kautta voi itse perustaa tarvittavia palvelimia, sekä hallinnoida palvelimen kapasiteettia, verkkoyhteyksiä ja palomuurauksia.

Tärkeä huomioitava asia on, että IaaS-mallissa palveluntuottajan vastuu ulottuu vain alustoihin, joita käytetään kapasiteetin tuottamiseen. Malli vaatii paljon osaamista ostajalta. Palvelunkäyttäjän vastuulle jäävät siis kaikki palvelimet, konfiguraatiot ja hallinnointi.

IaaS-palvelut sopivat hyvin organisaatiolle, jolla on oma IT-osasto tai -porukka tai tarvittavaa osaamista muuta kautta. Palvelun käyttäjä huolehtii siis itse palvelimien tietoturvasta, palomuurauksesta sekä asennuksista ja ohjelmistoista. [14]

4.5 PaaS – Platform as a Service

PaaSista puhutaan kun palveluntuottaja tarjoaa palveluna sovelluslustoja, jotka ovat paketoitu helposti käyttöön otettavaan muotoon. Sovelluslustoja tarjotaan yleisesti ottaen ohjelmistokehityksen käyttöön/tarpeisiin. Käytännössä palvelunkäyttäjä voi tilata sopivan alustan, maksaa joustavasti käyttöön perustuen ja siirtää sovelluksensa palveluun. [14]

Tyypillisesti PaaS-alustassa palveluntarjoaja tarjoaa web käyttöliittymän lisäksi vaihtoehtoisia tapoja muodostaa yhteyksiä palveluihin, kuten suorat yhteydet palvelimiin (FTP/SFTP, SSH), komentorivityökalut (CLI) ja API-rajapinta, jonka kautta voidaan automatisoida toimenpiteitä, ja tuoda palvelut osaksi omaa sovellusta tai itsepalvelumallia. [14]

PaaS laajentaa palveluntuottajan vastuulle myös käyttöjärjestelmä- ja varusohjelmisto-tasot. Palvelunkäyttäjän vastuulle jää oman sovelluksen tietoturva. Käytännössä tämä tarkoittaa sitä, että palvelunkäyttäjän tulee huolehtia itse sovellustason päivityksestä sekä tietoturvasta. [14]

Yksinkertaisimmillaan tämä tarkoittaa, että jos laitat PaaS-alustaan verkkosivut, jossa on alustana julkaisujärjestelmä (esimerkiksi WordPress, Drupal), huolehdi itse julkaisujärjestelmään liittyvistä päivityksistä ja tietoturvasta. [14]

Valmiiden sovelluslustojen käyttäminen tuo tehokkuutta, poistaa tarvetta omalle ylläpidolle, ja mahdollistaa ketterän kehityksen tukien ohjelmistokehityksen hyvien käytäntöjen mukaisia toimintamalleja. [14]

4.6 Microsoft Azure

Microsoft Azure on Microsoftin pilvipalvelu, jota voidaan käyttää sekä IaaS- että PaaS -alustana. Microsoft Azure skaalautuu käyttäjän tarpeen mukaan joko puhtaasti pilviratkaisuksi, tai se voidaan yhdistää osaksi paikallista IT-infrastruktuuria.

Microsoft on listannut yli 600 Azure -palvelua, joihin lukeutuu mm. data-analytiikkaa, tietokantoja, tallennustilaa ja verkkopalveluja. Käyttäjää laskutetaan jokaisesta palvelusta erikseen, ja käytettyjä Azure -palveluja voi hallita verkkopohjaisen Azure Portal -ohjelman avulla.

Microsoft Azure tukee useita eri ohjelmointikieliä ja ohjelmistoja, joista osa on kolmansien osapuolten kehittämiä. Azure tarjoaa esimerkiksi huomattavan valikoiman Linuxin kanssa yhteensopivia palveluita. [10]

Azure toimii pay-as-you-go-mallilla, jossa käyttäjää veloitetaan ainoastaan niistä resursseista jotka ovat olleet käytössä. Resursseja voidaan muokata lennossa. Azuren tukipalvelut on jaettu usealle

kohderyhmälle porrastetusti, ja sisältää kuukausimaksun. Perusversio on nimeltään Basic joka kuuluu oletuksena kaikkiin Azure-tileihin, mutta lisäksi tarjolla on myös maksulliset Developer (29\$/kk), Standard (100\$/kk), sekä Professional Direct (1000\$/kk) jäsenyydet. Lisäksi tarjolla on Premier-jäsenyys, jonka hintaa Microsoft ei suostu paljastamaan julkisesti. Tuen taso ulottuu Basicistä alkaen perinteisestä asiakaspalvelutuesta Azure-ammattilaisten vetämiin webinaareihin ja koulutukseen Premier-tasolla. [13]

4.7 Microsoft 365

Microsoft 365 on Microsoftin tarjoama palvelupohjainen toimistotyökalupaketti. Microsoft 365:n aiempi nimi oli Office 365. Pakettiin kuuluu aiempien Office-pakettien ydinohjelmistot Word, Excel, PowerPoint ja Outlook sekä yhteistyökalut kuten Sharepoint, Teams, Yammer. Kokonaisuuksia tarjotaan eri hintaisilla lisensseillä. Eri paketit tuovat mukanaan erilaisia palveluita kuten Exchange-serverin, tiedostonjako-palvelun sekä Active Directory-integraation. Palvelun vahvuuksiin kuuluu sen käyttäminen laitteistosta, ajasta ja paikasta riippumatta. [9]

Microsoft 365 Business Basic (aiemmin Office 365 Business Essentials)	Microsoft 365 Business Standard (aiemmin Office 365 Business Premium)	Microsoft 365 Business Premium (aiemmin Microsoft 365 Business)	Microsoft 365 -sovellukset yrityksille (aiemmin Office 365 Business)
4,20 € käyttäjä/kuukausi (vuositilaus) ALV ei sisälly hintaan.	10,50 € käyttäjä/kuukausi (vuositilaus) ALV ei sisälly hintaan.	16,90 € käyttäjä/kuukausi (vuositilaus) ALV ei sisälly hintaan.	8,80 € käyttäjä/kuukausi (vuositilaus) ALV ei sisälly hintaan.
Osta nyt	Osta nyt	Osta nyt	Osta nyt
Kampanjahinta näkyy ostoskorissa. ⁵	Kokeile maksutta yksi kuukausi ⁴	Kokeile maksutta yksi kuukausi ⁴	
Yrityksille, jotka tarvitsevat Microsoft Teamsin ja pilvitalennustilaa. Office-sovellusten työpöytäversiot eivät sisälly pakettiin.	Yrityksille, jotka tarvitsevat Office-sovellukset eri laitteisiin sekä yritys sähköpostin, tiedostojen pilvitalennustilaa, verkkokokoukset ja keskustelut.	Yrityksille, jotka tarvitsevat Business Standardin kaikkia ominaisuuksia sekä kehittyneen kyberhuojauksen ja laitehallinnan.	Yrityksille, jotka tarvitsevat Office-sovellukset eri laitteisiin ja tiedostojen pilvitalennustilaa. Ei sisällä yritys sähköpostia ja Microsoft Teamsia.
Sisältävät Office-sovellukset (Sisältää Wordin, Excelin ja PowerPointin verkko- ja mobiiliversiot.) ³	Sisältävät Office-sovellukset	Sisältävät Office-sovellukset	Sisältävät Office-sovellukset
Outlook Word Excel PowerPoint Publisher (vain PC) Access (vain PC)	Outlook Word Excel PowerPoint Publisher (vain PC) Access (vain PC)	Outlook Word Excel PowerPoint Publisher (vain PC) Access (vain PC)	Outlook Word Excel PowerPoint Publisher (vain PC) Access (vain PC)
Sisältävät palvelut	Sisältävät palvelut	Sisältävät palvelut	Sisältävät palvelut
Exchange OneDrive SharePoint Teams	Exchange OneDrive SharePoint Teams	Exchange OneDrive SharePoint Teams Intune Azure Information Protection	OneDrive

Microsoft 365 hinnoittelu. [24]

4.8 Azure Active Directory

Azure Active Directory on ilmainen pilvipohjainen autentikointipalvelu, jolla luodaan luottamussuhde paikallisen Exchange-organisaation, ja pilvessä sijaitsevan Exchange Online-palvelun välillä. Palvelu on pakollinen hybridimallissa, jossa aiotaan hyödyntää Office 365:ttä. Office 365:n lisenssejä

voidaan hallinnoida myös Azure AD:n kautta. Toiminnan vaatima trusti voidaan luoda manuaalisesti federaatiopalveluiden kautta, tai työkalun määrittelyvaiheessa Hybrid Configuration Wizardia hyödyntäen. Palvelun avainominaisuuksiin kuuluvat:

Password hash synkronointi – Kirjautumismetodi, joka synkronoi käyttäjän tunnukset molempiin hakemistoihin.

Pass-through autentikointi – Kirjautumismetodi, joka mahdollistaa samojen tunnusten käytön molemmissa hakemistoissa.

Federation integraatio – Azure AD Connectin valinnainen osa, jota hyödynnetään hybridimalleissa.

Tässä ratkaisussa käyttäjän autentikointi tapahtuu paikallisessa hakemistossa pilvihakemiston sijaan.

Tarjoaa myös sertifikaattipalvelun.

Synkronointi – Vastuussa käyttäjien, ryhmien ja muiden objektien luonnista. Huolehtii samalla identiteetti-informaation vastaavuudesta kummassakin hakemistossa.

Monitorointi – Azure AD Connect Health-palvelulla pystytään monitoroimaan palvelun tilaa Azure portalista.

Organisaatioiden hallinta tapahtuu yhteisesti Exchange 2016-serverin Exchange Admin Center-hallintakonsolissa. [10]

4.9 Autodiscovery

Exchange-palvelimelle luodaan asennuksen yhteydessä automaattisesti webbipalvelu, johon käyttäjät ottavat yhteyden halutessaan päästä postilaatikkoonsa käsiksi. Tämän palvelun avulla käyttäjän Outlook löytää sähköpostilaatikon määitykset automaattisesti, jotta käyttäjän ei tarvitse itse manuaalisesti määrittää niitä joka kerta kun sähköpostilaatikkoon halutaan päästä käsiksi. Prosessi lähtee Active Directoryn kautta liikkeelle. Käyttäjä kysyy hakemistolta SCP-objektia, joka sisältää Exchange-serverin, sekä autodiscoveryn osoitteen. SCP-objekteja on kahdenlaisia, SCP-pointtereita sekä SCP URL-osoitteita. SCP-pointterit osoittavat LDAP-serverille, joita käytetään objektien paikantamiseen. SCP URL-osoitteet sisältävät itse autodiscoveryn osoitteen. Osoite noudattelee usein yrityksen sähköpostin mallia esim.

<https://email.contoso.com/autodiscover/autodiscover.xml>. [7]

Autodiscoveryyn liittyy myös DNS-komponentti, joka toimii CNAME- ja .SRV-rekordien varassa.

CNAME-rekordi on käytännössä alias, joka liittää IP-osoitteen ja nimen yhteen.

Yrityksen käyttämässä DNS-palvelussa sijaitseva tyypillinen CNAME-rekordi voisi näyttää seuraavalta:

Name: autodiscover

TTL: 3600

RR Type: CNAME

Target: Exchange-serverin FQDN

Vaihtoehtoisesti määrittelyssä voidaan käyttää myös .SRV-rekordia, jolla voidaan määritellä tietyn protokollan, palvelun tai DNS-domainin sijainti. [7]

Yrityksen käyttämässä DNS-palvelussa sijaitseva tyypillinen .SRV-rekordi voisi näyttää seuraavalta:

Service: _autodiscover

Protocol: ._tcp

Port Number: 443

Host: mail.contoso.com

Priority: 0

Weight: 0

Lisäksi autodiscovery-palveluita tarjoavalle serverille on luotava oma DNS-rekordi, jotta Exchange-tilit toimivat Outlookissa oikein. Autodiscover tunnistaa käyttäjän sähköpostiosoitteen perusteella. Tämän jälkeen käyttäjän Outlook-client yhdistää URL-osoitteeseen, josta se vastaanottaa .xml tiedoston joka sisältää käyttäjänimen, yhteysasetukset sisä- ja ulko verkkoon sekä serverin jossa käyttäjän sähköpostilaatikko sijaitsee. Tietojen muuttuessa autodiscover päivittää .xml-tiedostoon sisältyvät tiedot automaattisesti. [7]

5 YMPÄRISTÖN LÄHTÖTILANNE

Suurimpaan osaan BFG:n servereistä on asennettu Windows 2008 tai 2012. Sähköpostipalvelut nojasivat projektin aloitushetkellä Exchange 2007-palveluun. Toimistotyökaluina yrityksellä on käytössä Office 2010-paketti, joten päivitys tuoreempaan Exchange-, sekä Office 365-palveluun on yrityksen kannalta selkeä askel nykyaikaisempaan, tuetumpaan sekä ennenkaikkea tuottavampaan ratkaisuun.

Järjestyksessä ensimmäisenä oli Active Directory-migraatio. Office 365 oli tulossa käyttöön kummankin AD:n käyttäjille, joten mainittu lähestymisjärjestys on looginen. AD migraatio toteutettiin siten, että ensin luotiin uusi AD-serveri tuoreeseen NPC-ympäristöön, jonne kaksi nyt käytössä olevaa AD:ta migroitiin trustien luomisen jälkeen. Tämän jälkeen siirryttiin migroimaan postilaatikot uuden ympäristön Exchange 2016-serverille. Tämän jälkeen postilaatikot synkattiin Azure Active Directorya hyödyntäen Office 365:n piiriin. Office 365-asennukset ja käyttöönotto pyrittiin toteuttamaan osastoittain, jotta mahdollisiin ongelmakohtiin oli helpompi tarttua, sekä niiden vaikutukset rajattua. Viimeisenä oli tarkoitus migroida palvelimet sekä laitteisto, mutta nämä jäivät toteuttamatta korona-pandemian vuoksi.

Teknisestä näkökulmasta nämä kaksi erillistä yritystä tuottivat päällekkäisiä palveluita, jotka oli huomioitava uuden rakenteen suunnittelussa. BFG:n vanhassa ympäristössä Active Directory oli rakennettu siten että polussa ensimmäisenä olivat eri toimipisteet, Suomessa, Tanskassa, Ruotsissa ja Hong Kongissa. Näiden alla olivat eri osastot, joihin kuuluvat johto, talous, design, myynti, varasto ja IT. Lisäksi VPG:n Active Directoryssa on vastaavia osastoja, joten Active rakenne oli tarkoitus yhtenäistää projektin edetessä. Myös tämä osio jäi kesken korona-pandemian vuoksi.

Työntekijöitä on BFG:n alaisuudessa noin 80 kpl, joista suurimmalla osalla on omia kannettavia, mobiililaitteita, tabletteja sekä käyttäjiä AD:hen yhdistettynä. AD-serverillä oli projektin alussa käytössä Windows 2008. Vanhan ympäristön käytössä oleva Exchange 2007-serveri sijaitsee virtuaalisena Tanskassa HyperV-ympäristössä.

Kaikille uusille käyttäjille asennettiin Office 2010-paketti aina laitteiston valmistelun yhteydessä. Tiedostojen jakamiseen käytettiin yrityksen tiedostoservereillä sijaitsevia kansioita, sekä esim. Dropbox-pilvipalvelua. Projektinhallintaa sekä tehtävienjakoa hoidettiin Wrike-verkkopalvelulla. Omalla intranetillä huolehdittiin yrityksen sisäisten asioiden uutisoinnista sisältäen mm. organisaatiokuvauksen, puhelinluettelon ja erinäisiä ohjeistuksia. Kaikkien näiden palveluiden tuki oli luonnollisesti hajautettu, sillä palveluita tuottavat eri tahot. Office 365 on yhtenäisempi ratkaisu, sillä palvelu tarjoaa laajan skaalan monipuolisia työkaluja Office 2010-pakettiin verrattuna. Lisäksi palveluiden tukea saatiin yhtenäistettyä osan palveluista siirtyessä Office 365:n piiriin.

6 PROJEKTIN KÄYTÄNNÖN TOTEUTUS

6.1 Suunnittelu

Migraatiojärjestykseksi valittiin käyttäjät, sähköpostilaatikat ja viimeisenä laitteisto. Oli selvää että käyttäjät oli migroitava ensin, sillä postilaatikat lukevat Active Directory-tunnuksia, joten käyttäjien migroiminen postilaatikoiden jälkeen ei ollut missään tapauksessa realistinen vaihtoehto. Laitteisto päätettiin jättää viimeiseksi, sillä käyttäjät ja sähköpostilaatikat koettiin tilanteen kannalta kriittisemmäksi. Lisäksi projektin laitteiston migroinnista ei oltu aloitusvaiheessa tehty vielä tarpeeksi taustatyötä, joten migraatio koettiin riskialttiiksi. Oli siis loogista aloittaa projekti käyttäjien migroinnilla ja siirtyä siitä postilaatikko-migraatioon, jättäen näin laitteiston viimeiseksi. Lisäksi ympäristön palvelimissa oli elinkaarikysymyksiä, jotka oli selvitettävä jotta varmistettaisiin migroinnin järkevyys. Ympäristöön kuului useita servereitä, joiden tuki oli joko loppunut, tai loppumaisillaan.

6.2 Uudet serverit

Projektin ensimmäisinä toimina rakennettiin servereitä uuteen ympäristöön. Näihin kuuluivat Active Directory, Exchange 2016 sekä vanhaan ympäristöön kaksi kappaletta identtisiä ADMT-servereitä täysin käyttäjä- sekä laitteistomigraatiota varten, yksi BFG:lle sekä toinen VPG:lle. Kaikki serverit lisättiin Tanskassa sijaitsevaan VPG:n hallinnoimaan HyperV-ympäristöön, jonka jälkeen servereille asennettiin alla mainitut palvelut.

Domain Controller/Active Directory

Windows Server 2012 R2, 4 ydintä, 8 gigatavua keskusmuistia, C-asema 80 gigatavua (*käyttöjärjestelmä*), D-asema 40 gigatavua (*Active Directory tietokanta*)

Exchange 2016:

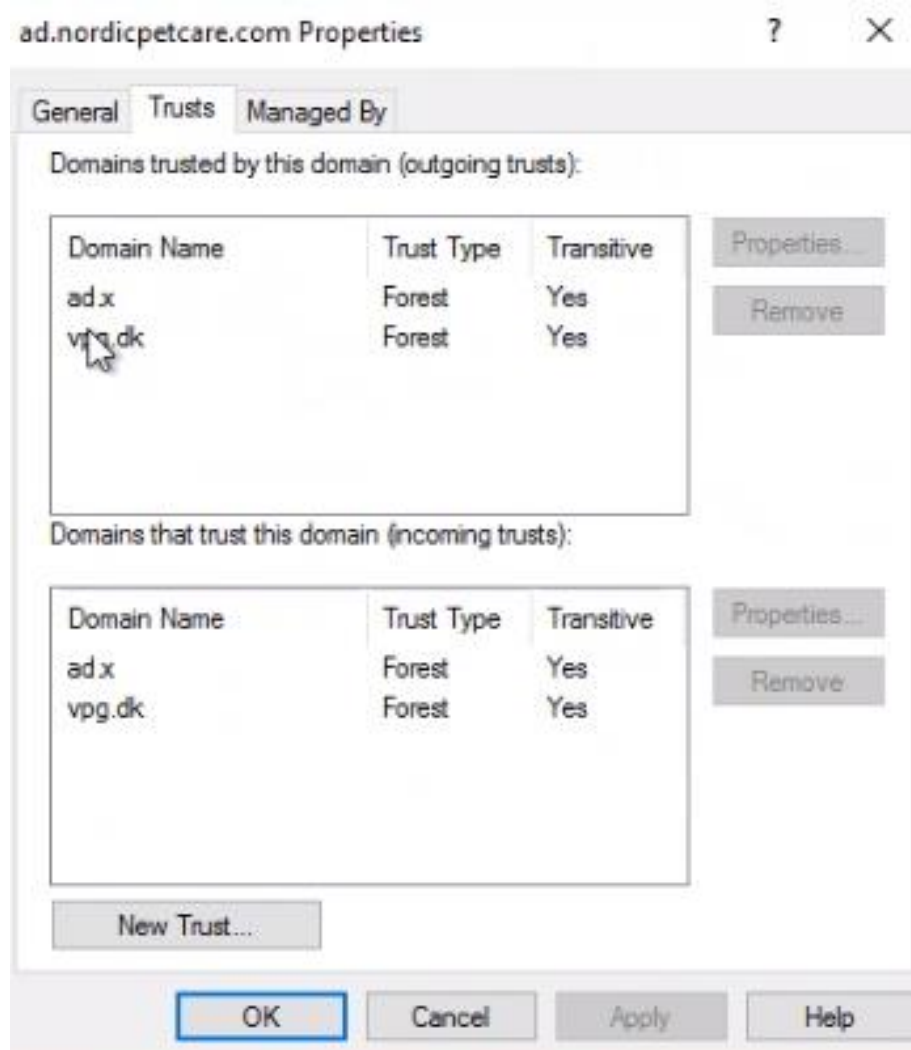
Windows Server 2012 R2, 4 ydintä, 32 gigatavua keskusmuistia, C-asema 80 gigatavua (*käyttöjärjestelmä*), D-asema 200 gigatavua (*Exchange logit*), E-asema 2500 gigatavua (*tietokannat*), F-asema 100 gigatavua (*Exchangen ja tietokannan muutoslogit*)

ADMT migraatioserveri (kaksi kappaletta)

Windows Server 2012 R2, 2 ydintä, 4 gigaa keskusmuistia, C-asema 100 gigatavua (*käyttöjärjestelmä, ADMT työkalu*)

6.3 Trustien rakentaminen

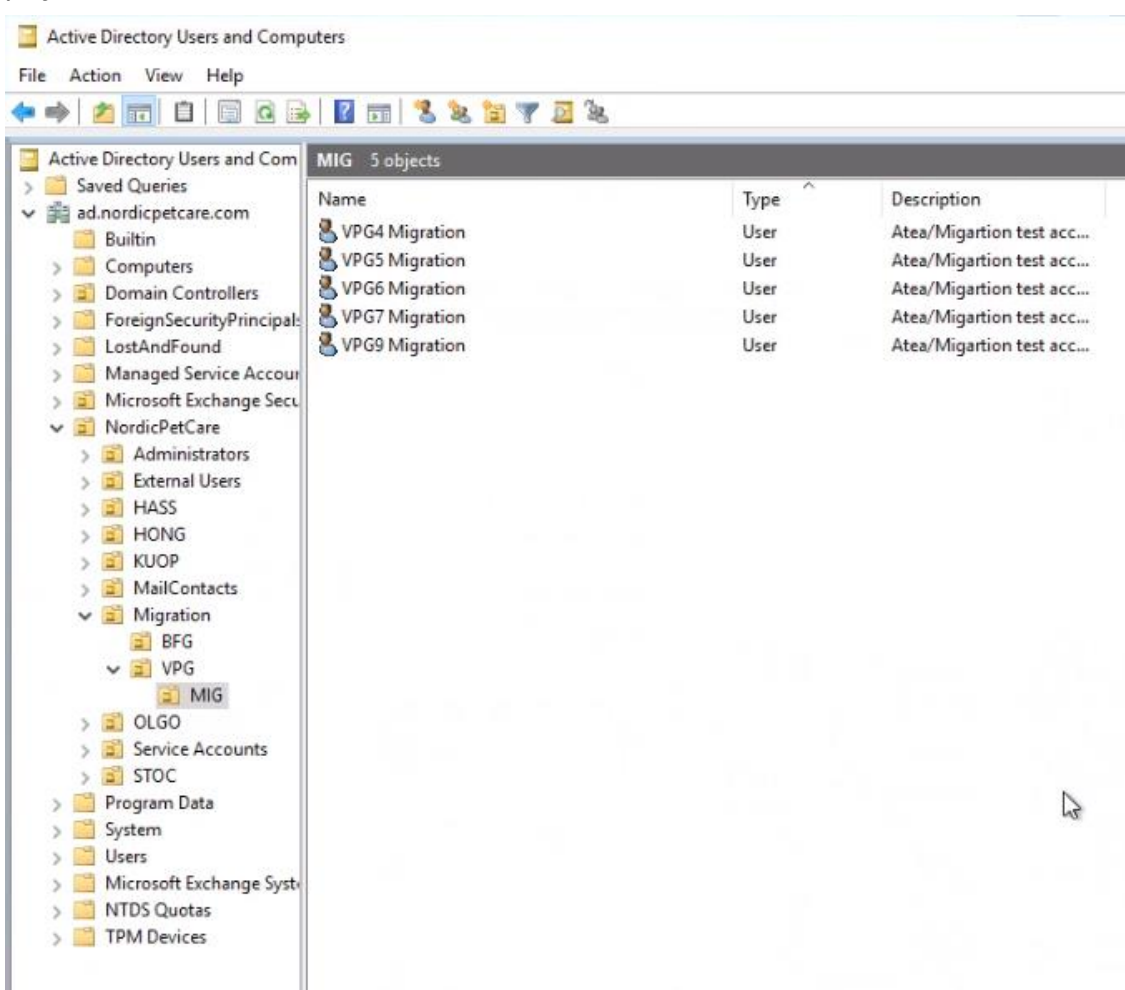
Palvelimien rakentamisen jälkeen seuraava askel oli luoda trustit BFG:n ja VPG:n domain controllereiden kanssa uuteen ympäristöön. Myös tämä oli erittäin selkeä askel sillä trustin muodostama yhteys on elinehto migraatioiden toteutukselle. Ilman trustia servereiden välinen autentikointi epäonnistuu, ja migraatiodata ei lähe replikoitumaan vanhasta ympäristöstä. Trustit luotiin erikseen ongelmitta Active Directory Domains and Trusts työkalun kautta. BFG:n ja VPG:n ympäristöjen välillä oli jo luottamussuhde sisaryhtiö-tilanteen takia, ja nyt molemmissa ympäristöissä oli luottamussuhde myös uuteen NPC-ympäristöön.



Trustit luotuna uuden ympäristön AD-serverille. Ad.x on BFG:n domain ja vpg.dk VPG:n.

6.4 Active Directory-migraatio

Seuraava askel oli käyttäjien migrointi uuteen ympäristöön. Migraatiossa hyödynnettiin ADMT-serverillä valmiiksi ollutta User Account Migration Wizardia, jossa määritettiin lähde-, sekä päämääräympäristö, sekä molempien ympäristöjen domain controllerit. Uudessa ympäristössä oli migraatiota varten luotu Organizational Unit, joka toimi migroitavien tunnusten päämääränä, josta käyttäjät siirrettäisiin manuaalisesti oikeisiin alihakemistoihin. Migroinnin yhteydessä oli mahdollista migroida joko vanhat salasanat, tai luoda uudet, ja tässä projektissa päädyttiin ensimmäiseen vaihtoehtoon. Käyttäjämäärä oli niin suuri, että oli loogista vähentää potentiaalisten uusien salasanojen tuomaa sekavuutta, ja tyytyä migroimaan vanhat salasanat myös uuteen ympäristöön. Samalla määritettiin käyttäjäryhmät siirtyväksi migraatiossa, sillä niitä ei ollut tarve muuttaa tässä projektivaiheessa.



Testikäyttäjää uuden ympäristön AD-palvelimella. Samalla kuvaa AD-rakenteesta.

6.5 Exchange-migraatio

Seuraavaksi siirryttiin postilaatikkomigraatioon, sekä kokoamaan listaa migroitavista käyttäjistä. Samalla tehtiin päätöksiä vanhemmista käyttäjistä, joita ei tulisi migroimaan uuteen ympäristöön. Näin saatiin siivottua käyttäjälistaa ennen migraation varsinaista alkamista. Käytännössä tehtävä suoritettiin siten, että Active Directory-palvelimelta haettiin PowerShell-skriptillä käyttäjiä joiden postilaatikko oli sillä hetkellä projektia käytössä. Näin saatiin lista käyttäjistä, joiden postilaatikko oli migraatiohetkellä käytössä. Samankaltainen skripti ajettiin disabled-tilassa oleville postilaatikoille,

luoden listan käyttäjistä joiden migroiminen uuteen ympäristöön oli syytä ottaa harkintaan. Skriptiin sisällytettiin listan ajo Excel-tiedostoihin, joiden pohjalta BFG:n tietohallinto tulkitsee dataa, ja arvioi migraatiosta pois jätettäviä käyttäjiä merkiten tiedon ylös tiedostoon. Käytetty skripti näytti siis seuraavalta:

```
Get-ADUser - Filter <Enabled -eq $true> / Select Name > c:/temp/kayttajalista.csv
```

Käytännössä migraatioprosessin ensimmäinen vaihe oli ajaa uuden ympäristön Exchange-serveriltä PowerShell-skripti, joka valmistelee postilaatikon migraatiota varten varmistaen samalla että migroitavan käyttäjän sähköpostilaatikko on olemassa ja sisältää tarvittavat AD-attribuutit. Skripti kopioi kyseiset attribuutit, ja luo niiden pohjalta uuden sähköpostikäyttäjän. Skriptiin määritellään migroitava identiteetti, vanhan sekä uuden ympäristön domain controllerit, sekä molempiin kirjautumistiedot tilistä, jolla on lupa kopioida tai kirjoittaa dataa omaan forestissaan. Skriptin pohja:

```
Prepare-MoveRequest.ps1 -Identity JohnSmith@Fabrikan.com -RemoteForestDomainController  
DC001.Fabrikam.com -RemoteForestCredential $RemoteCredentials -LocalForestDomainController  
DC001.Contoso.com -LocalForestCredential $LocalCredentials [18]
```

Jokaisella käyttäjällä oli migraation jälkeen käytössä "@migration.bestfriend.com" -mallinen sähköpostiosoite, jolla varmistettiin sähköpostin toimivuus uuden ja vanhan ympäristön sähköpostin välillä. Sähköpostin reititys oli määritetty yhdistimen avulla toimimaan vanhan ympäristön serverin kautta.

Exchangen lähetyshdistin - Internet Explorer

To Kuopsv01

Nimi:
To Kuopsv01

Yhdistimen tila:
☒ Ota käyttöön
☐ Välitä client access -palvelimen kautta

Kommentti:

Yhteyshäytännön lokiin kirjoituksen taso:
☐ Ei mitään
☒ Yksityiskohtainen

***Lähetettävän viestin enimmäiskoko (Mt):**
 35

Tallenna Peruuta

Sähköpostireititys toimi edelleen vanhan ympäristön KuopSrv01-serverin kautta.

Seuraavaksi suoritettiin varsinainen siirto. Palvelinasiantuntija määritteli skriptin siten, että migraatio suoritetaan 95% valmiiksi, ja kuitattiin myöhemmin manuaalisesti sopivana ajankohtana. Manuaalisella kuittauksella varmistettiin parempi kontrolli migraatiosta, sekä se toimi samalla vahvistuksena siitä, että postilaatikko on siirtynyt ongelmitta vanhasta ympäristöstä uuteen. Skriptiin määriteltiin identiteetin lisäksi migroitava Exchange-palvelin, tietokanta, sekä toimitusalue.

Tässä vaiheessa selvisi että migrointi Best Friendin Exchange 2007 serveristä uuteen ympäristöön ei onnistu suoraan, kuten alunperin oletettiin. Ongelmaksi muodostui fakta, että Exchange 2007:n tuki oli loppunut. Ratkaisuksi ehdotettiin migrointia Exchange 2013-versioon, josta sen jälkeen migroitaisiin Exchange 2016 versioon, luoden näin välittömän ratkaisun. HyperV-ympäristöön luotiin uusi Exchange 2013-serveri tehtävänään toimia migraation välivaiheena. Migraatio päätettiin toteuttaa viikonloppuna, sillä näin minimoitaisiin käyttäjien toiminnan katkeaminen. Salasana-asetukset muutettiin ennen migraatiota Group Policyn kautta "never expire" -tilaan mahdollisten konfliktien välttämiseksi, ja migraation jälkeisten ongelmien minimoimiseksi. Näin käyttäjien salasanat säilyivät samana myös uudessa ympäristössä.

6.5.1 Testaus

Migraatiotestaus aloitettiin luomalla testikäyttäjää sähköpostilaatikoineen. Käyttäjät luotiin yrityksen yleisiä tapoja noudattaen, eli Exchange 2007:n kautta luotiin sähköpostilaatikko, joka sisälsi skriptin, jolla käyttäjälle luodaan myös AD-tunnus. Käyttäjille lisättiin kalenterimerkintöjä, sekä pääsy muutamiin sähköpostilistoihin. Näin simuloitiin aidon tilin tilannetta. Ensin testattiin paikallisen käyttäjän tilanne siirtämällä postilaatikko Exchange 2007:sta Exchange 2013:n kautta Exchange 2016:een, kuten työssä on aiemmin mainittu. Testattava postilaatikko lakkasi toimimasta Exchange 2013-serverillä Outlookin mukaan, mutta seuraavan siirron jälkeen Outlook löysi uudet määritelmät Exchange 2016-serveriltä, ja testaus todettiin onnistuneeksi.

Samalla suoritettiin mobiilitestausta, jossa ryhmä lisäsi testikäyttäjän tunnukset oman mobiililaitteen sähköpostisovellukseen. Sähköpostilaatikko toimi ilman ongelmia, joten myöhemmin suoritettiin muuten identtinen testi, mutta tällä kertaa käytössä olleella laitella oli koko testin ajan VPN-yhteys päällä. Näin saatiin huomioitua myös etäkäyttäjien tilanne, joka BFG:n tapauksessa muodostuu lähinnä toimiston ulkopuolella työskentelevistä myyjistä, sekä joistakin työntekijöistä joiden avainrooleihin kuuluu matkustaminen. Tämänkin testauksen tulos oli positiivinen, sillä VPN-yhteydelläkin testikäyttäjän Outlook tunnisti muutokset, ja otti ne käyttöön onnistuneesti.

6.5.2 Mobiililaitteiden migrointi

Mobiililaitteiden migraatio osoittautui ongelmalliseksi, sillä BFG:llä ei ollut keskitettyä mobiilihallintaa, ja laitteita oli noin 80. Tämä tarkoitti käytännössä, että mobiililaitteet olisi migroitava manuaalisesti joko itse käyttäjien, tai tietohallinnon toimesta. Käyttäjien tueksi päätettiin kirjoittaa kuvallinen ohje, jossa neuvottiin mobiililaitteelle tehtävät muutokset, jotka suoritettaisiin migraation jälkeen.

Käytännössä käyttäjän piti navigoida laitteellaan sähköpostisovelluksen palvelinasetuksiin, ja muuttaa tunnukseen liitetyn toimialueen nimi, sekä palvelin itsenäisesti.

DNA 4G 48 % 14.20

Saapuvan postin asetukset

Sähköpostiosoite
matti.meikäläinen@bestfriend.com

Toimialueen nimi
nordicpetcare

Käyttäjänimi
fimme

Salasana
.....

Palvelin
outlook.nordicpetcare.com

Portti
443

Suojaustyyppi SSL/TLS >

= aiemmin ad tai ad.x

= aiemmin mail.bestfriend.com

Lisäksi käyttäjiä rohkaistiin olemaan yhteydessä IT-tukeen, mikäli muutokset tuottivat ongelmia. Kaikki laitteisto saatiin lopulta uuden ympäristön piiriin, joko itsenäisesti tai tietohallinnon toimesta. Muutosten tekeminen ei lopulta aiheuttanut läheskään niin suurta päänvaivaa, kuin tietohallinto ennakoi mobiilihallinnan puutteen noustessa esille.

6.5.3 Kannettavien migrointi

Kannettavat tietokoneet vaativat käyttäjältä ainoastaan hyväksynnän palvelinmuutoksesta Outlookin sisällä. Lisäksi sähköposti oli testattu toimivaksi verkkoportaalien kautta, joten käyttäjillä oli siis olemassa varavaihtoehto, jos migraatio olisi jostain syystä epäonnistunut heidän kohdallaan.

6.5.4 Migraation jälkeiset ongelmat

Aivan täysi menestys sähköpostimigraatio ei kuitenkaan ollut. Jälkeenpäin alkoi esiintyä ikäviä jälkivaikutuksia, sillä ryhmäsähköpostit, sekä kalenterit eivät toimineet kuten piti. Käyttäjät eivät

pystyneet tekemään kalenterivarauksia toistensa kalentereihin, ja isommat sähköpostilistat lakkasivat tyystin toimimasta. Lisäksi ryhmäsähköpostit eivät kulkeutuneet osalle käyttäjistä, tai niiden käyttö saattoi olla eväty. Sähköpostilistat saatiin toimimaan ajamalla niille Exchange 2016-serverillä LegacyDN-attribuutti taaksepäin sopivuuden takaamiseksi. Tämä suoritettiin hakemalla LegacyDN-arvot vanhan ympäristön AD-serveriltä Excel-tiedostoon, ja ajamalla ne uuden ympäristön AD-serverille AD-moduulin käyttökehoitteita hyödyntäen. Tämän jälkeen osa listoista alkoi taas toimimaan Outlookissa normaalisti.

Ongelmaan perehtyminen paljasti lisää. Migraation jälkeen uuden ympäristön Active Directory-hakemisto oli erilainen kuin vanhassa ympäristössä. Vanhasta ympäristöstä migroitiin yksittäiseen migraatiota varten luotuun OU:hun uudessa ympäristössä, josta käyttäjät oli tarkoitus siirtää oikeisiin alihakemistoihin. Käyttäjien sijainti uudessa ympäristössä ei enää vastannut vanhaa, ja tämä oli pääsyy ongelmiin.

Erityiseksi ongelmaksi muodostui Hasselagerin toimisto, sillä hakemistoon kuului alunperin käyttäjiä sekä BFG:n että VPG:n puolelta, ja migraation alkuvaiheessa oli vielä tarve eritellä käyttäjät omiin listoihin erinäisten ilmoitusten vuoksi. Uuden ympäristön sähköpostilista toimi kuitenkin siten, että molempien yritysten käyttäjät olivat samassa listassa, joten oli mahdotonta lähettää sähköpostia ainoastaan BFG:n tai VPG:n Hasselagerin käyttäjille, vaan viesti meni kaikille Hasselagerin toimistossa.

Eräs sähköpostilista vastaanotti muutosten jälkeen postia ulkopuolisesta verkosta, mutta ei näkynyt sisäisessä osoitekirjassa. Palvelinasiantuntija ehdotti että Office 365:n jaettu postilaatikko voisi tällaisessa tilanteessa olla hyvä ratkaisu sillä se ei vie lisenssiä, mutta antaa usealle käyttäjälle pääsyn samaan postilaatikkoon.

6.6 Sähköpostin uudelleenreititys

Postilaatikoiden migraation jälkeen alettiin pohtia sähköpostin uudelleen reititystä. Tavoitteena oli siirtää myös sähköpostin reititys uuden Exchange-serverin piiriin. Exchange 2007-tuki oli loppunut ja ympäristö hyödynyi tässä vaiheessa edelleen vanhaa Exchange 2007-serveriä SMTP-palveluiden reitittämiseen sekä roskapostifiltteriin. Tehtävä jäi kesken korona-pandemian takia.

6.7 Office 365 migrointi

Office 365 käyttöönoton valmistelevat toimenpiteet aloitettiin ennen Active Directory-hakemiston migraation suorittamista, sillä alkutoimenpiteet eivät häirinneet AD- tai postilaatikko-migraatiota millään tavoin. Ensimmäisenä askeleena Office 365-tilauksen jälkeen lisättiin NPC:n domain palveluun hallintapaneelin kautta. Tämän jälkeen oli vahvistettava domainin omistajuus DNS-rekordien avulla. Vahvistamiseksi päätettiin käyttää .TXT-recordia, joka saatiin DNS-palveluntarjoajalta. Käytännössä ensin kirjauduttiin palveluntarjoajan sivustolle, jonne rekordi ensin lisättiin. Tämän jälkeen Office 365-hallintapaneelistä suoritettiin käsky etsiä .TXT-recordia jolla

vahvistettiin omistajuus. Seuraavaksi lisättiin MX-rekordi, jolla määritettiin Office 365-palvelut vastaanottamaan uutta postia vanhan serverin sijaan. Tämän jälkeen lisättiin CNAME-rekordit autodiscoverille, jotta käyttäjät löytävät uudet määritykset automaattisesti.

Seuraavan rakennettiin ADConnect-serveri jonka tehtävänä on synkronoida paikallisen Active Directory-hakemiston objektit pilvessä sijaitsevaan vastaavaan hakemistoon Office 365 käyttöä varten. Serveri on pakollinen Office 365:n toiminnan kannalta hybridiympäristössä. Käytännön perspektiivistä kyseessä oli työkalu, joka asennettiin uudelle serverille kuten mikä tahansa muu ohjelma. Ennalta vaadittiin ainoastaan Azure AD-tilaus, joka kuuluu vakiona Office 365-tilaukseen. Työkalun asennuksen yhteydessä siihen määritettiin Azure-tunnukset, sekä paikallinen AD synkronointia varten, ja se määritettiin alkamaan välittömästi asennuksen jälkeen.

Synchronization Service Manager on AZUREADCONNECT

File Tools Actions Help

Operations Connectors Metaverse Designer Metaverse Search

Name	Profile Name	Status	Start Time	End Time
ad.nordicpetcare.com	Export	success	1/27/2020 8:12:55 AM	1/27/2020 8:12:55 AM
nordicpetcare.onmicrosoft.com - AAD	Export	success	1/27/2020 8:12:48 AM	1/27/2020 8:12:54 AM
nordicpetcare.onmicrosoft.com - AAD	Delta Synchronization	success	1/27/2020 8:12:48 AM	1/27/2020 8:12:48 AM
ad.nordicpetcare.com	Delta Synchronization	success	1/27/2020 8:12:47 AM	1/27/2020 8:12:47 AM
nordicpetcare.onmicrosoft.com - AAD	Delta Import	success	1/27/2020 8:12:43 AM	1/27/2020 8:12:47 AM
ad.nordicpetcare.com	Delta Import	success	1/27/2020 8:12:42 AM	1/27/2020 8:12:43 AM
ad.nordicpetcare.com	Export	success	1/27/2020 7:42:54 AM	1/27/2020 7:42:54 AM
nordicpetcare.onmicrosoft.com - AAD	Export	success	1/27/2020 7:42:47 AM	1/27/2020 7:42:53 AM
nordicpetcare.onmicrosoft.com - AAD	Delta Synchronization	success	1/27/2020 7:42:47 AM	1/27/2020 7:42:47 AM
ad.nordicpetcare.com	Delta Synchronization	success	1/27/2020 7:42:47 AM	1/27/2020 7:42:47 AM
nordicpetcare.onmicrosoft.com - AAD	Delta Import	success	1/27/2020 7:42:42 AM	1/27/2020 7:42:46 AM
ad.nordicpetcare.com	Delta Import	success	1/27/2020 7:42:42 AM	1/27/2020 7:42:42 AM
ad.nordicpetcare.com	Export	success	1/27/2020 7:12:54 AM	1/27/2020 7:12:54 AM
nordicpetcare.onmicrosoft.com - AAD	Export	success	1/27/2020 7:12:47 AM	1/27/2020 7:12:54 AM
nordicpetcare.onmicrosoft.com - AAD	Delta Synchronization	success	1/27/2020 7:12:47 AM	1/27/2020 7:12:47 AM
ad.nordicpetcare.com	Delta Synchronization	success	1/27/2020 7:12:47 AM	1/27/2020 7:12:47 AM
nordicpetcare.onmicrosoft.com - AAD	Delta Import	success	1/27/2020 7:12:42 AM	1/27/2020 7:12:46 AM
ad.nordicpetcare.com	Delta Import	success	1/27/2020 7:12:42 AM	1/27/2020 7:12:42 AM

Profile Name: User

Step Type: Partition: Start Time: End Time: Status:

Synchronization Statistics

Connection Status

Synchronization Errors

2088 run(s)

Käyttäjien synkronoinnin vahvistus AADConnect-serveriltä katsoen.

6.8 Office 365 käyttöönotto

Käyttäjien synkronoiduttua pilveen alettiin ottaa Office 365-ohjelmistoa käyttöön. Lisenssihallinta päätettiin hoitaa Azure AD:n kautta, jonne luotiin käyttäjäryhmä, jolla oli oikeus käyttää Office 365 tuotteita. Synkronoinnin ansiosta tämä ryhmä ilmestyi myös paikalliseen hakemistoon. Lopulta haluttu käyttäjä lisättiin paikallisessa hakemistossa haluttuun ryhmään, ja toisen synkronointivaiheen jälkeen Azure AD tunnisti käyttäjän lisäyksen. Lisenssi siirtyi näin käyttöön ja Office 365 voitiin asentaa käyttäjälle.

6.8.1 Office 365-lisenssit

Lisenssityyppejä oli käytössä kaksi. Suurin osa toimistokäyttäjistä siirrettiin käyttämään Microsoft 365-lisenssiä, kun taas varaston jaetuille käyttäjille määritettiin Office 365 Premium-lisenssi. Tämä

siksi, että varaston koneita käytettiin lähinnä kalenterivarauksiin sekä sähköpostitoimintoihin, joten oli selvää että käyttäjät eivät hyödy laajemmasta paketista. Microsoft 365 sisältää yrityssovelluksia sekä erinäisiä suojia, jotka ovat yksityisille kannettavaa laitteistoa hyödyntäville henkilöstölle tärkeitä, mutta eivät tuo merkittävää lisäarvoa varaston pakettikoneille. Microsoft 365 sisältää Office 365 Advanced Threat Protection ja Windows Exploit Guard Enforcement-suojat jotka tarjoavat molemmat Malware turvaa. Uhka todettiin kuitenkin pieneksi, sillä varaston sähköpostit eivät ole yleisessä jakelussa.

Yksi projektin haasteista liittyi Office 365-lisenssien jakamiseen. BFG:n varastolla on yhdeksän konetta, joita työntekijät käyttävät yhteisesti. Näihin koneisiin on liitetty kaksi jaettua sähköpostilaatikkoo, joista kuusi kuuluvat "Varasto" -nimiselle käyttäjälle, ja loput kolme "Pakkaamo" -nimiselle käyttäjälle. Yhden käyttäjän laitteistoraja on asetettu Office 365:ssä viiteen, joten "Varasto"-käyttäjän sähköpostilaatikoille täytyi keksiä jonkinlainen ratkaisu, jotta toiminta jatkuisi varastolla normaalisti. Keskustelujen yhteydessä oli selvää, että jatkossakin kaikilla varaston työntekijöillä tulisi olla yhteinen pääsy "Varasto" -käyttäjän sähköpostiin. Palvelinasiantuntijan vahva suositus oli, että jokaiselle varaston työntekijälle otettaisiin käyttöön oma lisenssi.

6.8.2 Asennus

Asennus aloitettiin kirjautumalla Office 365-portaaliin käyttäjän omilla tunnuksilla, ja lataamalla sieltä asennuspaketti. Käyttöönotto päätettiin suorittaa osastoittain kriittisimmistä aloittaen, jotta mahdollisiin ongelmiin voitiin reagoida rajatusti sekoittamatta niihin koko käyttäjäkuntaa. Kaikki asennukset suoritettiin kuitenkin kuukauden sisällä toisistaan.

Asennusten tyypillisen luonteen ansiosta ne onnistuivat suuremmista ongelmista, oli ainoastaan muistettava odottaa synkronointia lisenssiryhmään lisäyksen jälkeen. Tietohallinnon täytyi käydä suorittamassa asennus jokaisen käyttäjän laitteella erikseen keskitetyn hallinnan puutteen vuoksi, mutta tehtävää joudutti se, että asennuksia voitiin suorittaa monta yhtäaikaan latauksen ja itse asennusprosessin viedessä oman aikansa käyttäjän laitteiston jouhevuudesta riippuen.

6.8.3 Käyttäjien opastus

Samassa yhteydessä voitiin opastaa käyttäjiä yleisimpien Office 365-työkalujen käytössä. Aikaisempiin pakettiin kuuluneet ohjelmistot kuten Word, Excel ja PowerPoint olivat käyttäjille jo entuudestaan tuttuja, mutta esimerkiksi Teamsin käyttöönotossa tarvittiin opastusta, jota tietohallinto antoi omaan tietotaitoonsa nojaten. Tietohallinto havainnoikin, että käyttäjät näkivät heti erityisesti Teamsin potentiaalinen työympäristössä sekä työtehokkuuden parantamisessa.

6.8.4 Käyttöönoton jälkeiset ongelmat

Vaikka asennukset sujuivat pääsääntöisesti ongelmitta, osa ongelmista selvisi vasta jälkeenpäin. Toistaiseksi tuntemattomasta syystä OneDriven käytössä esiintyi useampaa käyttäjää vaivaava

ongelma, jossa OneDrive katosi laitteistolta, eikä ollut missään vaiheessa käyttökelpoinen. Ongelmaa lähdettiin korjaamaan asentamalla ohjelmisto uudelleen, mutta vika toistui jälleen.

6.9 Group Policy Object-päivitykset

Koska projektissa oli kyse kahden yrityksen yhdistymisestä, oli tarpeellista yhtenäistää joitain päällekkäisiä palveluita, joita yrityksen ovat erillään tuottaneet. Yksi näistä oli myös GPO:t. Päällekkäisten palveluiden lisäksi GPO "logiikkaa" oli yhtenäistettävä, sillä molempia oli rakennettu pitkällä aikavälillä useiden eri työntekijöiden toimesta, jotka eivät ole olleet keskenään tekemisissä. Molempien yritysten GPO:t käytiin läpi palaverin välityksellä, josta kerättiin dokumentoiden uuteen ympäristöön lisättävät yhtenevät policyt.

Samalla huomattiin useita policyjä jotka olivat nyky-ympäristön kannalta vanhentuneita, ja joita ei näin ollen tulisi luomaan uudelleen. Pääosin uuteen ympäristöön päätettiin luoda policyt, jotka liittyivät osastoihin, kansiojakoihin tai sähköpostiryhmiin. Jätettiin pois useita policyja jotka liittyivät ohjelmistoihin, joita yrityksillä ei ollut enää vuosiin käytössä. Kysymysmerkiksi jäi sijaintipohjaiset policyt, sillä vaikka kyseessä on projektin jälkeen yksi yritys, on sillä edelleen työntekijöitä useissa lokaatioissa ja neljässä eri maassa.

7 KORONAN VAIKUTUKSET

Tässä vaiheessa korona-pandemia jarrutti projektia siten, että projektiryhmä joutui siirtämään resursseja muihin työkohteisiin. Koska yritystä kehoitettiin työskentelemään etänä, fokusta siirrettiin väliaikaisesti kohti etäpalveluiden sujuvoittamista ja arkitoiminnan takaamista sillä oli selvää, että siihen liittyviä palveluita tulisi kuormittamaan tulevana kuukausina. Erityisesti Remote Desktop-resursseja pyrittiin lisäämään. Tämä toteutettiin poistamalla ja skaalaamalla alaspäin HyperV-ympäristössä olevia servereitä, vapauttaen näin lisäresursseja toimintojen takaamiseksi.

Ongelma heijastui erityisesti VPG:n puolella, jossa Remote Desktop-palvelu oli selkeästi ylikuormitettu. Tilaajan kannalta oli onni, että Office 365-työkalut saatiin sisäisesti kunnolla käyttöön ennen pandemian alkamista, sillä tuoreista toimistotyökaluista oli epäilemättä hyötyä työskentelyn siirtyessä pääsääntöisesti etätoteutukseen.

Resurssien jakautuessa muihin kriittisimpiin kohteisiin käytännönosion seuraavat kohdat on käsitelty tässä työssä teoreettisesti.

7.1 Laitteistomigraatio

Laitteistomigraation testausta aloitettiin ennen resurssien siirtämistä. Käytännöstä katsoen migraatio toteutettaisiin hyvin identtisin metodein kuin Active Directoryn käyttäjämigraatio. Tämä tarkoittaa sitä, että Microsoftilla on valmiiksi tarjota työkalu, ADMT, jolla laitteisto voidaan migroida yksinkertaista käyttäjäliittymää hyödyntäen. Tämä metodi sisältää myös lähes identtiset määrittelyt

käyttäjämigraatioon verraten. Työkaluun määritellään lähde- ja kohdedomainit, migroitavat laiteobjektit, sekä kohde OU, jonne objektit sijoitetaan uudessa domainissa. Kuten käyttäjämigraatiossa, domainien välillä on oltava olemassa trusti, ja tämä oli yksi ensimmäisistä toimista joita projektissa tehtiin. Pohjatyötä laitteistomigraatiota varten on siis käytännössä tehty jo aiemmin. Vaihtoehtoisesti migraatiossa voidaan käyttää myös PowerShellä, jos halutaan enemmän kontrollia sekä sisällyttää argumentteja, joita ADMT-työkalussa ei kysytä. [15]

Migroitavat kohteet voidaan määritellä joko hakemalla niitä hakemistosta, tai määrittelemällä .txt-tiedosto, johon kohteet on listattu yksi kerrallaan omille riveilleen vähintään kahta eri kenttää hyödyntäen. Näihin kuuluvat SourceName (nimi tai polku, jolla objekti löytyy hakemistosta) sekä TargetRDN (kohdenimi, jota uudessa hakemistossa käytetään objektista.)

Yksittäisiä kohteita migroitaessa voidaan käyttää hakua, mutta migroitaessa useita kohteita on järkevämpää tuottaa .txt-tiedosto nopeuden ja paremman kontrollin vuoksi. Lisäksi .txt-tiedostolla saadaan jonkinlainen referenssi migroitavista kohteista, jos tilannetta halutaan tarkastella myöhemmin. [15]

On syytä huomata että migraation yhteydessä laitteisto-objektit eivät lakkaa olemasta vanhassa domainissa, toisin kuin käyttäjämigraatiossa. Käytännössä objektit jäävät siis elämään vanhaan ympäristöön vielä migraation jälkeenkin, ellei niitä erikseen poisteta.

7.2 Exchange Online-migratio

Ennen koronan vaikutusta projektissa jäätiin tilanteeseen, jossa yrityksen sähköpostilaatikat sijaitsivat edelleen paikallisessa on-premise ympäristössä, josta Office 365 luki niitä Azure Active Directorya hyödyntäen. Yksi projektin tavoitteista oli siirtää postilaatikat paikallisesta on-premise ympäristöstä täysin pilveen, siirtyen näin vahvemmin pilviratkaisuun lakkauttaen paikallisen Exchange-serverin tarpeen.

Ensimmäisenä migraatioprosessissa luodaan Exchange Onlinen päässä endpoint hyödyntäen tiliä, jolla on oikeudet hallinnoida paikallista Exchange-serveriä. Endpointin määrittelyyn sisältyy käytännössä sähköposti, tilin domain sekä käyttäjänimi ja salasanan tilille. Tämä löytyy Exchangen hallintapaneelista kohdan Recipients -> Migration -> Migration Endpoints kohdan alta. Samalla määritellään migraation tyyppi, sekä migroidaanko Exchange Onlineen vai on-premise ympäristöön. [16]

Seuraavaksi otetaan käyttöön MRSProxy-endpoint paikallisella Exchange-serverillä, jos sitä ei ole vielä käytössä. Normaalisti serveri ei hyväksy replikointipyyntöjä turvallisuussyistä, ja tällä palvelulla serveri määritetään hallitusti hyväksymään replikointipyyntöt. Kyseinen endpoint on syytä poistaa käytöstä onnistuneen migraation jälkeen tietoturvasyistä. [17]

Hallintapaneelistä valitaan kohta Servers -> Virtual Directories. Tämän jälkeen valitaan Exchange-serveri, joka on yleensä muodossa "EWS Default Website", ja sen alta valitaan "Enable MRSPProxy endpoint." Tämän jälkeen voidaan vielä kirjoittaa Exchange Management Shelliin käsky *"Get-WebServicesVirtualDirectory / Format-Table -Auto Identity,MRSPProxyEnabled"*. Jos käsky palauttaa tuloksen "True", tulisi MRSPProxyn olla onnistuneesti käytössä. [16]

Seuraavaksi paikallisen Exchangen hallintapaneeli luodaan siirtojoberi Office 365 -> Recipients -> Migration kohdan alta, josta valitaan uusi jobi ja "Migrate to Exchange Online." Jobin luomisen yhteydessä määritellään migraation tyyppi sekä käyttäjät. Kuten muissakin migraatioissa, jobi vaatii onnistuakseen kirjautumistiedot hallintatilitille jolla on oikeus muokata ympäristöä. Migraation endpointtia vahvistaessa paneelin tulisi näyttää paikallisen Exchange serverin FQDN.

Tämän jälkeen määritellään kohdedomain migraatiolle, ja se on yleensä pääasiallinen SMTP-domain jota Exchange Onlinen sähköpostilaatikat käyttävät. Ne noudattavat usein muotoa "contoso.mail.onmicrosoft.com". Samalla voidaan vahvistaa että pääasiallisen sähköpostilaatikon lisäksi migroidaan myös arkisto-sähköpostilaatikko, joka käytännön tasolla tarjoaa käyttäjälle lisää tallennustilaa. Tämän jälkeen voidaan aloittaa migraatiojobi. [16]

7.3 Serverimigraatio

Viimeisenä työvaiheena tarkoitus oli migroida loput servereistä palveluineen uuteen ympäristöön samalla päivittäen mahdollisia servereitä ylöspäin tuetumpiin versioihin. Suurin osa tilaajan ympäristöstä muodostuu Windows 2008-servereistä, joista olisi suotavaa päästä hiljalleen eroon. Migroitaessa näistä versioista Windows 2016 tai 2019-servereihin on huomioitava, että osa palveluista ei migroidu suoraan, vaan vaatii ensin serverin päivityksen vanhassa ympäristössä tuetumpaan versioon, jotta migraatio uuteen versioon onnistuu. On siis varauduttava että osa servereistä joudutaan päivittämään vanhassa ympäristössä Windows 2008-versiosta esim. Windows 2016-versioon, josta sen jälkeen migroidaan serveri palveluineen uuteen ympäristöön. Windows 2008 R2 ei tue suoraan migraatiota aliverkkojen yli, joten näiden servereiden päivittäminen vähintään Windows 2012 versioon ennen migraatiota vaikuttaa erittäin todennäköiseltä.

Palveluiden yksityiskohtaista migraatiotukea on tarjolla hajautetusti. Tiedostopalvelimen migrointi Windows 2019 versioon on tehty erittäin helpoksi tuoreen Storage Migration Service-palvelun myötä. Verkkoselaimen pohjalla toimiva käyttöliittymä on nykyaikainen, ja vaatii lähde- ja kohdeservereiden lisäksi erillisen laitteiston käyttöliittymän hallinnointiin, sekä useita servereitä migroitaessa oman Windows 2019-serverin joka hallinnoi migraatiotyötä. Migraatio voidaan toteuttaa myös PowerShellin kautta. [20]

Muita palveluita migroitaessa migraatiometodit muuttuvat palvelusta toiseen, ainoa yhdistävä tekijä on Windows Server Migration Tools-työkalu, joka saadaan asennettua ominaisuutena "Add Roles and Features Wizard"-asennustyökalun kautta kohdeserverille. Käyttö tapahtuu jotakuinkin siten, että ensin ominaisuuden asentamisen jälkeen luodaan kohdeserverille kansio, johon

migraatiotyökalu asennetaan. Tämä kansio kopioidaan sen jälkeen lähdeserverille, jossa se rekisteröidään Command Promptissa käyttöön. Tämän jälkeen migraatiotyökalu on valmis käyttöön.

Työkalu on käskykehote-tyylinen, joten migroitava palvelu määrittää käskyt joita kehotteessa käytetään. Pääsääntöisesti palveluiden migraatio vaatii kuitenkin Windows Server Migration Toolsin asentamisen etukäteen, ja käskyt itsessään ovat import/export-tyylisiä, joihin määritellään migroitava palvelu, sekä lähde- ja kohdeserverit. On olemassa myös poikkeuspalveluita, joissa työkalua ei tarvita ollenkaan, vaan migraatioon vaaditaan esim. .xml-tiedoston vienti serveriltä toiselle, ja käyttöönotto PowerShellillä kuten verkkokäytäntöjen yhteydessä. Migraation määrittelyt on kuitenkin aina tarkistettava palvelukohtaisesti.

Linux-servereitä migroitaessa on muutamia asioita joita on syytä ottaa huomioon. On hyvä ajatus pyrkiä pitämään palveluiden versiot identtisinä lähde- ja kohdeservereiden kesken migraation helpottamiseksi. Suojatun tietoliikenneprotokollan, kuten SSH:n määrittäminen servereiden välille on elinehto migraation onnistumiselle. Kohdeserveri valmistellaan luomalla sinne vaatimusten mukaiset ominaisuudet lähdeserverin versioiden pohjalta. [22]

Itse migraatio voidaan suorittaa skriptillä, joka rakennetaan vaatimusten mukaisesti. Olennaisin skriptiin sisältyvä käsky on rsync, johon määritellään lähdeserveri, sekä lähde- ja kohdekansio. Käskyä käytetään pääasiassa automatisoitujen jobien, sähköpostien sekä ääritystiedostojen siirtoon. Jos tiedostoihin tarvitsee tehdä muutoksia, ne voidaan sisällyttää skriptiin suoraan. On kuitenkin huomioitava, että kyseisellä metodilla skripti tulitaisiin todennäköisesti ajamaan useamman kerran. [23]

Käyttäjätribuuttien migraatio vaatii työtä, sillä jokaiselle käyttäjälle määritetään Linuxissa ID-arvo, ja nämä eivät välttämättä vastaa toisiaan ympäristöissä. On siis olennaista selvittää migroitavalta serveriltä missä menee järjestelmäkäyttäjien, ja peruskäyttäjien raja ID:n suhteen. [23]

8 POHDINTA

Tämän työn tavoitteena oli dokumentoida, sekä toteuttaa Best Friend Group Oy:lle suunniteltu yritysfuusiosta aiheutuva ympäristöpäivitys. Lopputuloksena saatiin ympäristö, jossa on onnistuneita elementtejä tavoiteympäristöstä, mutta projektia ei kyetty viemään loppuun aikarajan puitteissa. Syynä tähän on korona-pandemia, sillä projektiryhmän toimiessa yritysten IT-tukena resurssit oli suunnattava muihin tehtäviin, jotta toiminta pystyttäisiin takaamaan etätöntehtäjiä ajatellen. Tämä ei sinänsä vaikuttanut dokumentointiin muuten, kuin että projektin loppuun suunnitellut käytännön tehtävät käsiteltiin teoreettisesti.

Aikataulun lipsumisesta huolimatta työ eteni alun aikataulumuutoksen jälkeen hyvää tahtia. On huomioitava että kukaan työryhmästä ei ole suorittanut tällaista projektia aiemmin. Tämä toi epäilemättä projektiin omat haasteensa, jotka on otettava huomioon projektia arvioidessa. Projektin statuspalaverit suoritettiin englanniksi Tanskan Hasselagerissa sijaitsevan projektijäsenen

vuoksi, ja kielitaidon jakautuessa palaverissa ymmärrettiin toisinaan sama asia eri tavoin, eikä tarkentavia kysymyksiä osattu aina kysyä, jotta päästäisiin kirkkaasti samalle aaltopituudelle. Kommunikointia harjoiteltiin siis käytännössä koko projektin ajan.

Lisäksi työskentelytavan oppiminen ryhmän kesken otti oman aikansa, kuten missä tahansa uudessa projektissa. Viikottaiset palaverit tarjosivat kuitenkin opinnäytetyön tekijälle mitä mainioimman mahdollisuuden muiden osallisten työn dokumentointiin. Dokumentointia onnistuttiin täydentämään myös erillisillä palaverilla, joihin asiantuntijat pyydettiin selvittämään tarkemmin omia toimiaan.

Teknisellä tasolla esiintyi ongelmia joita ei osattu ennakoida projektin edetessä. Nämä vaihtelivat pakollisista tehtävistä sivuongelmiin. Ongelmia ratkottiin priorisoiden pyrkien saavuttamaan piste, jossa projektia edistäviä toimia voitaisiin jatkaa.

Itse projektin dokumentointi on toimenä hyödyllinen, mutta on huomioitava että ympäristön lähtötila alkaa olla siinä määrin vanhentunut, että se rajoittaa epäilemättä tämän dokumentin hyödyllisyyttä. Näin laajan ympäristöpäivityksen peruskuvaus on hyödyllinen toimi, mutta se ei sovellu suoraan tuoreemman ympäristön migraatiopohjaksi, sillä esim. tuoreempien servereiden mukana ilmestyy uusia nyansseja, joita tässä työssä ei pystytä huomioimaan. Spekuloin perusprosessin kuvauksesta olevan kuitenkin hyötyä muille samankaltaista projektia toteuttaville henkilöille. Tuloksena syntynyt dokumentti toimii kuitenkin resurssina Nordic Petcare Groupin tietohallinnolle mahdollisissa ongelmanratkaisutilanteissa.

9 LÄHTEET JA TUOTETUT AINEISTOT

- [1] Migrate email using the Exchange cutover method. Verkkodokumentti.
<<https://docs.microsoft.com/fi-fi/Exchange/mailbox-migration/cutover-migration-to-office-365?redirectSourcePath=%2fen-us%2farticle%2fCutover-migration-to-Office-365-9496e93c-1e59-41a8-9bb3-6e8df0cd81b4>> Haettu 9.9.2019
- [2] Plan and Execute an Active Directory Merger, Part 2. Verkkodokumentti
<<https://www.itprotoday.com/active-directory/plan-and-execute-active-directory-merger-part-2>> Haettu 9.9.2019
- [3] How To: Interforest Migration Using Active Directory Migration Tool. Verkkodokumentti.
<<http://techgenix.com/interforest-migration/>> 24.9.2019
- [4] Perform a staged migration of email to Office 365. Verkkodokumentti
<<https://docs.microsoft.com/fi-fi/Exchange/mailbox-migration/perform-a-staged-migration/perform-a-staged-migration?redirectSourcePath=%252ffi-fi%252farticle%252fs%25c3%25a4hk%25c3%25b6postin-vaiheistettu-siirto-Office-365-ee-83bc0b69-de47-4cc4-a57d-47e478e4894e#prepare-for-a-staged-migration>> Haettu 24.9.2019
- [5] Best Friend Group. Verkkosivusto.
<<http://www.bestfriendgroup.com/fi/>> Haettu 10.1.2020
- [6] Active Directory Domain Services Overview. Verkkodokumentti.
<<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>> Haettu 1.10.2019
- [7] AD DS Design Requirements. Verkkodokumentti.
<<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/ad-ds-design-requirements>> Haettu 1.10.2019
- [8] Overview of Exchange services on Exchange servers. Verkkodokumentti.
<<https://docs.microsoft.com/en-us/exchange/plan-and-deploy/deployment-ref/services-overview?view=exchserver-2019>> Haettu 1.10.2019
- [9] Microsoft 365 for enterprise overview. Verkkodokumentti.
<<https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-overview?view=o365-worldwide>> Haettu 8.11.2019
- [10] What is Azure AD Connect? Verkkodokumentti.
<<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect>> Haettu 8.11.2019
- [11] Exchange Server hybrid deployments. Verkkodokumentti.
<<https://docs.microsoft.com/en-us/exchange/exchange-hybrid>> Haettu 8.11.
- [12] M365 vs. O365 Licensing Explained. Verkkodokumentti.
<<https://getnerdio.com/academy/m365-vs-o365-licensing-explained/>> Haettu 15.11.2019
- [13] Compare support plans. Verkkodokumentti.
<<https://azure.microsoft.com/en-us/support/plans/>> Haettu 15.11.2019
- [14] IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi. Verkkodokumentti.

<<https://www.planeetta.fi/2016/03/15/iaas-paas-saas-mika-pilvipalvelu-sopii-yrityksellesi/>> Haettu 20.3.2020

[15] Intraforest Migration in Windows Server 2016 with Active Directory Migration Tool (ADMT) 3.2 Verkkodokumentti.

<<https://www.starwindsoftware.com/blog/intraforest-migration-in-windows-server-2016-with-active-directory-migration-tool-admt-3-2>> Haettu 24.9.2019

[16] Move mailboxes between on-premises and Exchange Online organizations in hybrid deployments. Verkkodokumentti.

<<https://docs.microsoft.com/en-us/exchange/hybrid-deployment/move-mailboxes>> Haettu 12.11.2019

[17] How to create a migration endpoint Exchange Online. Verkkodokumentti.

<<http://www.thatlazyadmin.com/how-to-create-a-migration-endpoint-exchange-online/>> Haettu 3.5.2020

[18] Understanding the Importance of MRS Proxy in Hybrid Deployment Model Office 365. Verkkodokumentti.

<<https://gallery.technet.microsoft.com/Understanding-the-0c8ce203/file/156810/1/Understanding%20the%20Importance%20of%20MRS%20Proxy%20in%20Hybrid%20Deployment%20Model.pdf>> Haettu 3.5.2020

[19] Prepare mailboxes for cross-forest moves using the Exchange Management Shell. Verkkodokumentti.

<<https://docs.microsoft.com/en-us/exchange/architecture/mailbox-servers/prepare-mailboxes-for-cross-forest-moves-in-powershell?view=exchserver-2019>> Haettu 2.12.2019

[20] Storage Migration Service overview. Verkkodokumentti.

<<https://docs.microsoft.com/en-us/windows-server/storage/storage-migration-service/overview>> Haettu 4.5.2020

[21] Windows Server Migration Common Tasks and Information. Verkkodokumentti.

<[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff400258\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff400258(v=ws.10))> Haettu 28.9.2020

[22] How To Migrate Linux Servers Part 2 - Transfer Core Data. Verkkodokumentti.

<<https://www.digitalocean.com/community/tutorials/how-to-migrate-linux-servers-part-2-transfer-core-data>> Haettu 4.5.2020

[23] How To Migrate Linux Servers Part 3 - Final Steps. Verkkodokumentti.

<<https://www.digitalocean.com/community/tutorials/how-to-migrate-linux-servers-part-3-final-steps>> Haettu 4.5.2020

[24] Microsoft 365 tuoteperheet. Verkkodokumentti.

<<https://www.microsoft.com/fi-fi/microsoft-365/compare-all-microsoft-365-products?&activetab=tab:primaryr2>> Haettu 25.5.2020